Unlocking Data Accuracy & Security: Macro Global's Key to The UK Bank's FSCS SCV Reporting Success

macro global®
creating value through innovation

SA SF

Table of Contents

macro global®
creating value through innovation

SA
SF

Table of Contents

Client Overview

A leading bank in the UK encountered significant shortcomings in its Single Customer View (SCV) reporting. Inconsistent and inaccurate data plagued their SCV/Exclusion files, compromising the accuracy of reports submitted to the Prudential Regulation Authority (PRA). This posed a serious threat to regulatory compliance and potentially hefty fines. Additionally, the lack of robust data security measures during transmission to the cloud server exposed sensitive customer information to potential breaches.

Considering the gravity of these challenges, the bank ran for a reliable partner to address their data woes. They approached Macro Global, a leading provider of SCV reporting solutions, with the intent to leverage their expertise and technology to cleanse their data and streamline the reporting process. Macro Global's proven record of accomplishment in data governance, customer data validation, and regulatory compliance made them the ideal partner for the bank to navigate these data challenges and achieve successful FSCS SCV reporting.

How Macro Global Helped the UK Bank Get Through SCV Reporting Challenges?

Challenge 1: Ensuring Data Quality for Flawless SCV/Exclusion Reporting

The bank faced significant challenges in ensuring data quality within its SCV (Single Customer View) and Exclusion files before submitting them to the PRA (Prudential Regulation Authority). These data inconsistencies restricted precise reporting and potentially threatened the bank's compliance with regulatory requirements. It includes:

1.1 Missing or Incomplete Information

The SCV/Exclusion files of the bank contain missing information for critical fields like customer name, address components, date of birth, account details (BIC, UK Company Registration Number, Product Type), and account holder indicator. This lack of data created an incomplete picture of depositors and their holdings, hindering accurate customer identification and reporting.

1.2 Data Privacy and Protection

The bank suffered from the challenge of inadequate security measures and improper control mechanisms in managing and protecting customer data within the SCV system. This led to vulnerabilities that escalated the chance of unauthorised access, potential data breaches, monetary setbacks, and reputational damage.

1.3 Data Duplication

The bank's system identified duplicate entries within the files, including duplicate customer information including customer name, date of birth, address, passport number, email address, phone number, potentially leading to inaccurate reporting and skewed analysis, making it difficult to track individual customer information.

1.4 Inaccurate Account Holder and Customer Information

Inaccurate information such as incorrect account holder indicator, invalid account status code, special characters, or unusual characters within customer details within the bank's SCV report led to miscommunication, missed opportunities, and difficulties in identifying eligible depositors for FSCS protection.

1.5 Inaccurate Account Segregations

Inaccurate segregation like exclusion type value present in the SCV file, data format issues, or invalid "structured deposit account" flag prevents proper classification of accounts (SCV vs. Exclusion) and can lead to reporting errors with the PRA.

1.6 Poor Data Aggregation

The UK bank struggles to integrate and structure data from various sources effectively, hindering the creation of a holistic customer profile. This fragmented data view and inconsistent data formats like customer name in address fields, incorrect postcode formats limit the bank's ability to generate insightful reports and make informed decisions.

Solution Implemented

Three-phase Solution to Address Data Challenges

Phase 1

Gap Analysis and Strategy Deployment

- SMEs and business professionals conducted an operational and business readiness assessment.

- Identified the client's need for a comprehensive approach to data governance.

Phase 2

Strategy Deployment

- Recommendations for improved data standards were forwarded to the client.

- Framework implementation was carried out, including data-related decisions, processes, and controls.

- Processes and business rules were defined for ongoing governance and common standard data definitions were developed.

Phase 3

Implementation

- The client's current data model was integrated with MG's Data Governance framework using industry-leading platforms like SCV Forza and SCV Alliance, to improve data architecture, master data management, and data warehousing.

3.1 Automating SCV Report Generation with FSCS SCV Audit & Automation Suite

The FSCS SCV Audit & Automation solution improved data quality, operational readiness, and accuracy in FSCS SCV Regulatory reporting:

Data Screening:

The SCV Forza engaged only cleansed data for SCV output generation using gap study and staging area data.

Upholding Security:

Data privacy and protection are ensured by keeping all SCV-related information in the SCV server, with output files only accessible to authorised users. Data duplication is managed using fuzzy logic validations and mechanisms.

Eliminating Inaccurate Data:

Inaccurate customer and account holder information's are removed from the staging area to comply with minimum data requirements in SCV files.

Ensuring Compliance:

All FSCS specified standards are strictly followed within the SCV automation platform, resulting in high-level accuracy and full compliance.

Data Validation:

Inaccurate reporting and less informed decisions are avoided by ensuring successful validations and mandatory conditional validations.

Effective Segregation:

Account segregations are managed using linked accounts and relationship datasets, ensuring data integration.

Efficient Aggregation:

Data aggregation is managed by the SCV Forza – FSCS SCV Automation intelligent platform, ensuring accurate reporting to FSCS satisfaction.

3.2 Third-Party Integrations for Enhanced Data Validation

Third-party integrations of trusted databases like FCA, Loqate, Companies House, BFPO Dataset, OFAC Sanction Dataset and Charities Register provided reliable solutions for data verification as detailed below:

FCA Register:

Returns non-individual customer details if a company's registration number or company name does not match with the FCA Register dataset.

Companies House/ Charities Register:

Returns non-individual customer details with invalid UK company number or company name or number if it does not match with "UK Companies House Registry or Charities Register".

Multiple Entities under One SCVRN Number:

Extracts company names with joining terms, matches them with the company's house registry, and reports any matching part names in the exception report.

BFPO Dataset:

Returns incorrect positioning of BFPO address, verifies BFPO number reporting position and country field emptiness if the address is BFPO.

Loqate Dataset:

Returns UK customer addresses, invalid postcodes, or incorrect postcode formats.

UK and OFAC Sanction Dataset:

If any customer has BFPO address then this validation checks the BFPO address with BFPO dataset and report if the BFPO number or postcode is invalid.

3.3 Steps Involved in Automated SCV Reporting

Automated SCV reporting solutions rely heavily on customer data validation, which verifies, corrects, and enhances customer information in real time and four stages comprise the process, which include:

Data Mining:

Checks and updates client information, including name, address, phone number, email address, and account number, against trusted international data sources. This guarantees consistent, reliable, and comprehensive data from multiple sources.

Data Cleansing:

Employs deduplication logic to eliminate or correct inaccurate, obsolete, and corrupt entries from a dataset. This process streamlines disorganised data and reduces the occurrence of reporting errors.

Data Enrichment:

Ensures compliance with regulations by adding missing or insufficient data points to the existing information, improving its quality.

Data Reconciliation:

Involves the verification and alignment of information from various origins to guarantee precision and consistency. Automating this comparison procedure reduces manual work and errors, maintaining the accuracy and integrity of the financial records.

Outcome

Macro Global's SCV audit and automation solutions promoted the bank's SCV reporting, guaranteeing data integrity in the following ways:

- Turned PRA's RED rating into GREEN with no penalties.

- Restored immunity with continuous business operations.

- Enhanced the bank's data insight and strengthened customer relationships.

- Addressed long-standing systematic issue, redefining reporting with Regulatory Reporting Hub.

- Enhanced data accuracy and consistency by preventing human error and auto-synchronising data across platforms.

- Improved credibility of data by accessing reliable information from trusted sources.

- Deterred fraudulent activities by verifying real-time data against reliable databases.

- Strengthened capacity to meet regulatory mandates for KYC responsibilities.

- Improved operational efficiencies by automating repetitive data tasks and reducing manual intervention.

- Ensured enhanced compliance with regulatory requirements through built-in features and automated data management.

- Automated data gathering, validation, and consolidation, minimising errors and ensuring adherence to reporting deadlines.

- Improved efficiency, enhanced risk management, fostered transparency and accountability, and led to operational savings due to reduced manual effort and improved data quality.

Challenge 2: Securing SCV Reporting Data in Transit

Ensuring the confidentiality of data transmitted from the bank's network to the SCV cloud server for regulatory reporting appeared to be challenging. As this data possesses sensitive customer information, robust encryption measures were mandatory to prevent unauthorised access and potential breaches.

Solution Implemented

To address the bank's security concerns, a secure data transmission solution leveraging Microsoft Azure is implemented. The workflow involves:

Azure Key Vault:

A secure cloud-based service was deployed to store and manage the encryption keys used to protect the bank's data. This centralised key management system ensures strict access controls and eliminates the risk of unauthorised key usage.

Encryption and Decryption Logic:

Encryption logic is integrated into bank's systems to encrypt data before transmission to the SCV cloud server. Upon reaching the server, decryption logic ensures authorised access for processing and reporting purposes.

Outcome

By implementing MG's solutions, the bank achieved significant improvements in data security for their SCV reporting:

- Encryption safeguards sensitive customer data, minimising the risk of network breaches.

- Access controls ensure only authorised personnel access to encryption keys.

- Robust encryption measures demonstrate the bank's data security compliance.

- Provides peace of mind for data transmission.

macro global®
creating value through innovation

Conclusion

Macro Global offers a compelling value proposition for the bank seeking to optimise their Single Customer View (SCV) reporting processes.

The successful partnership between the UK bank and Macro Global showcases the benefits of collaborating with an experienced data governance and SCV reporting expert. Macro Global's SCV Forza and SCV Alliance are specialised solutions with well-architected data model, designed to tackle diverse challenges faced by organisations in SCV reporting.

SCV Forza and SCV Alliance solutions provided scalability for the bank to handle data volumes of any size, ensuring future proofing as data grows. The highly customisable API and well-optimised reporting application enabled seamless integration within existing data environments.

With over 70 years of combined expertise, Macro Global's consultants offered invaluable insights and ensured data quality and integrity. Integrations with trusted sources allowed for comprehensive data screening, while risk classification flags helped to prioritise remediation efforts.

Benchmarking capabilities and actionable insights of SCV solutions supported continuous improvement, and regulatory compliance reporting ensured adherence to FSCS requirements. Generic Plug-in APIs facilitated easy integration with core banking systems, and thus, Macro Global offered complete support throughout the FSCS journey, providing a supportive and comprehensive experience for the UK bank.

By unifying customer data across internal systems and capturing customer activities across all channels through Macro Global's solutions - SCV Forza & SCV Alliance, the bank achieved enhanced data security, improved data quality, streamlined reporting processes, flawless regulatory compliance, informed decision-making, and enhanced customer engagement.

macro global®
creating value through innovation

We are here to help you

Please click on the web link below to access our sales desk telephone numbers and email and we will be in touch straight back to you.

🌐 https://www.macroglobal.co.uk/contact-us/

macro global
creating value through innovation

Macro Global (MG) is the trading name of Macro Infotech Limited, Inca Infotech Ltd & Macro Technology Solutions Pvt Ltd. Macro Infotech Limited & Inca Infotech Limited have Registered Office at 25, Cabot Square, Canary Wharf, London – E14 4QZ and these companies are registered in England & Wales under the registration number 06477763 & 04017901.

Technology Partnerships

Microsoft Gold Partner

amazon web services | Partner Network
TECHNOLOGY PARTNER

trust payments

kaleyra

ISO Certifications

| ISO 9001:2015 Quality Management System Cert. #: 0922900102 | ISO 27001:2013 Information Security Management Cert. #: 09222700102 | ISO 27701:2019 Privacy Information Management Cert. #: 09222770102 | ISO 27018:2019 PII Protection in Public Clouds Cert. #: 09222701802 |